UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/805,761	03/22/2004	Tanna Marie Richardson	SLA1564	1251

7590 05/17/2007

Gerald W. Maliszewski
P.O. Box 270829
San Diego, CA 92198-2829

EXAMINER	
SHAN, APRIL YING	
ART UNIT	PAPER NUMBER
2135	
MAIL DATE	DELIVERY MODE
05/17/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/805,761	RICHARDSON, TANNA MARIE	
	Examiner	Art Unit	
	April Y. Shan	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 March 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4,7-13 and 16-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4, 7-13 and 16-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. The Applicant's amendment, filed 05 March 2007, has been received, entered into the record, respectfully and fully considered.

2. As a result of the amendment, claims 1-2, 7, 9-11, 16 and 19 have been amended. Claims 5-6 and 14-15 are canceled. Claims 1-4, 7-13 and 16-19 are now presented for examination.

Claim Rejections - 35 USC § 112

3. Claims 7-8 and 19 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

As per claims 7-8 and 19, the claim limitation "**comparing the access code to the hashed password**" is not enabling. According to the abstract of the original disclosure, the Applicant discloses "**compares the hashed password to the hashed access code**". How can a not hashed access code compared to a hashed password and find match? *In re Wands, 858 F. 2d 731, 737, 8 USPQ2D 1400, 1404 (Fed. Cir. 1998).*

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 1-4 and 7-8 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As per **claim 1**, "transmitting...encrypted document data" is being recited. It is not clear "encrypted document data" is the same as or different from "encrypting the scanned document" recited in line 6 of claim 1.

Any claim not specifically addressed, above, is being rejected as incorporating the deficiencies of a claim upon which it depends.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

8. Claims 1-4, 7-13 and 16-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hutchison (U.S. Publication No. 2003/0145218) in view of McGraw (U.S. Patent No. 6,542,261)

As per **claims 1 and 10**, Hutchison discloses a method/system, comprising:

at a source, scanning a document ("In a digital copier, wherein hard-copy original images are scanned...." – e.g. abstract and fig. 1);

accepting a password ("...such as by entering passwords...." – e.g. paragraph [0024] and paragraph [0026]);

encrypting the scanned document ("original data is encrypted before being stored in the memory..." – e.g. abstract); and,

transmitting the encrypted document with the password (e.g. in paragraph [0021], Hutchison discloses "...In particular, the method known as "Pretty Good Privacy" or "PGP" uses a "**session key**"...which is itself encrypted using a public key and **sent to a recipient**..." and in paragraph [0025], Hutchison discloses "PGP then creates the session key, which is a random number typically derived from incidental data" and "In a sense, an entered **password** or other identification is a type of incidental data useful in random number generation" in the paragraph [0025] of Hutchison.), from the source to a network-connected printer (in paragraph [0014], Hutchison discloses "...**network-controlled** printer" and in paragraph [0013] and in fig. 2, Hutchison discloses "Fig 2 is a diagram of a set of digital copiers and associated computers arranged on **a network**..." And in paragraph [0029], Hutchison discloses "a plurality of digital copiers 10 are

connected, through known means such as one or more subnetworks 72, 74 connected through a router 76...")

- Hutchison does not disclose expressly hashing the password.

However, Hutchison discloses using Pretty Good Privacy (PGP) as the basic encryption technique (e.g. paragraph [0025]). It is well known in the art at the time of the invention that PGP uses MD5 as a one-way hash function. Additionally, Hutchison discloses in paragraph [0025], "using PGP, the original data is compressed according to any one of known techniques,...this is a typical step in digital copying anyway".

At the time of the invention it would have been obvious to a person of ordinary skill in the art to replace the encrypted password with the hashed password or to incorporate a hashed password in the Hutchison's method/system and transmit the encrypted document to a network-connected printer, with the password, includes transmitting the encrypted document with the hashed password.

The motivation of doing so would have been "compression is a typical step in digital copying anyway...not only reduces of amount data that must be encrypted, but also would confound many straightforward cryptological attack techniques", as taught by Hutchison (paragraph [0025]) and "protecting such data within a copier, or more broadly, within any system in which image data is scanned and retained for subsequent printing", as taught by Hutchison (paragraph [0003]).

- Hutchison does not disclose a file including:

an unencrypted header with an identification of the scanned document.

McGraw discloses wherein transmitting the encrypted document with the hashed password includes transmitting a file including: an unencrypted header with an identification of the scanned document (e.g. fig. 4, abstract and col. 3, lines 6-11).

Hutchison and McGraw are analogous art because they are from the same field of endeavor of digital copier. At the time of the invention it would have been obvious to a person of ordinary skill in the art to incorporate McGraw's unencrypted header to Hutchison's method/system.

The motivation for doing so would have been since "The printed or viewed received FAX will have the unencrypted header at the top of the page so that the receiving party (who may not be the intended recipient) will know to whom the received secure FAX document should be given to. For example a hotel's business center would need to know which guest the secure FAX should be delivered to", as taught by McGraw (col. 3, lines 6-11).

As per **claims 2 and 11**, Hutchison-McGraw discloses a method/system as applied above in claims 1 and 10. Hutchison further discloses comprising:

at the printer, accepting the encrypted document and password (paragraph [0021] and paragraph [0025]. Please note in paragraph [0021], the session key is itself encrypted and sent to the recipient.);

accepting an access code at a local interface ("...by entry of a suitable password or identification at UI 22" – e.g. paragraph [0027]);

comparing the access code to the password ("only a "correct" code would provide access to a private key" – e.g. paragraph [0027]);

in response to a matching the access code to the password, decrypting the document (e.g. paragraph [0025], [0027]); and,

printing the decrypted document (e.g.abstract).

As per **claims 3 and 12**, Hutchison-McGraw discloses a method/system as applied above in claims 1 and 10. Hutchison further discloses wherein accepting a password includes accepting a password selected from the group including a PIN number, an alphanumeric code, biometric data, Smart card, magnetic stripe card, and proximity badge (paragraph [0024]).

As per **claims 4 and 13**, Hutchison-McGraw discloses a method/system as applied above in claims 2 and 11. Hutchison further discloses wherein encrypting the document includes: at the source, deriving an encryption key from the password (e.g. paragraph [0022], [0025] and [0026]); and,

using the encryption key to encrypt the document (e.g. paragraph [0022], [0025] and [0026]).

As per **claims 7 and 16**, Hutchison-McGraw discloses a method/system as applied above in claims 2 and 11. Hutchison further discloses comprising: at the printer, entering the access code (paragraph [0027]; and, wherein comparing the access code

to the password includes comparing the password to the access code (paragraph [0027]).

Hutchison does not disclose expressly hashing the access code and wherein comparing the access code to the password includes comparing the hash password to the hashed access code.

However, Hutchison discloses using Pretty Good Privacy (PGP) as the basic encryption technique (e.g. paragraph [0025]). It is well known in the art at the time of the invention that PGP uses MD5 as a one-way hash function. Additionally, Hutchison discloses in paragraph [0025], "using PGP, the original data is compressed according to any one of known techniques,...this is a typical step in digital copying anyway".

At the time of the invention it would have been obvious to a person of ordinary skill in the art to incorporate a hashed access code in the Hutchison's method/system and compare the access code to the password includes comparing the hash password to the hashed access code.

The motivation of doing so would have been "compression is a typical step in digital copying anyway...not only reduces of amount data that must be encrypted, but also would confound many straightforward cryptological attack techniques", as taught by Hutchison (paragraph [0025]) and "protecting such data within a copier, or more broadly, within any system in which image data is scanned and retained for subsequent printing", as taught by Hutchison (paragraph [0003])

As per **claims 8 and 17**, Hutchison - McGraw discloses a method/system as applied above in claims 7 and 16. Hutchison further discloses wherein decrypting the document includes:

regenerating the encryption key from the access code (paragraph [0027]); and,

using the encryption key to decrypt the encrypted document (paragraph [0027]).

As per **claim 18**, Hutchison-McGraw discloses a system as applied above in claim 11. Hutchison further discloses wherein the printer user interface accepts an access code selected from the group including a PIN number, an alphanumeric code, biometric data, Smart card, magnetic stripe card, and proximity badge (e.g. paragraph [0027]).

As per **claims 9 and 19**, Hutchison discloses a method/system for recovering scan to confidential print communications, the method comprising:

at a network-connected printer interface ("...it is conceivable that the present invention can be embodied in a combination of separate devices....network-controlled printer..." – e.g. paragraph [0014], paragraph [0029] and fig. 1, 2), accepting a file including an encrypted document and password (e.g. in paragraph [0021], Hutchison discloses "...In particular, the method known as "Pretty Good Privacy" or "PGP" uses a "**session key**"...which is itself encrypted using a public key and **sent to a recipient**..." and in paragraph [0025], Hutchison discloses "PGP then creates the session key, which is a random number typically derived from incidental data" and "In a sense, an entered

password or other identification is a type of incidental data useful in random number generation" in the paragraph [0025] of Hutchison.), from the source to a network-connected printer (in paragraph [0014], Hutchison discloses "...**network-controlled** printer" and in paragraph [0013] and in fig. 2, Hutchison discloses "Fig 2 is a diagram of a set of digital copiers and associated computers arranged on **a network**..." And in paragraph [0029], Hutchison discloses "a plurality of digital copiers 10 are connected, through known means such as one or more subnetworks 72, 74 connected through a router 76...")

accepting an access code at a local interface ("...by entry of a suitable password or identification at UI 22" – e.g. paragraph [0027]);

comparing the access code to the password ("only a "correct" code would provide access to a private key" – e.g. paragraph [0027]);

in response to a matching the access code to the password, decrypting the document (e.g. paragraph [0025], [0027]); and,

printing the decrypted document (e.g. abstract).

- Hutchison does not disclose expressly the password is hashed password.

However, Hutchison discloses using Pretty Good Privacy (PGP) as the basic encryption technique (e.g. paragraph [0025]). It is well known in the art at the time of the invention that PGP uses MD5 as a one-way hash function. Additionally, Hutchison discloses in paragraph [0025], "using PGP, the original data is compressed according to any one of known techniques,...this is a typical step in digital copying anyway".

At the time of the invention it would have been obvious to a person of ordinary skill in the art to replace the encrypted password with the hashed password or to incorporate a hashed password in the Hutchison's method/system and transmit the encrypted document to a network-connected printer, with the password, includes transmitting the encrypted document with the hashed password.

The motivation of doing so would have been "compression is a typical step in digital copying anyway...not only reduces of amount data that must be encrypted, but also would confound many straightforward cryptological attack techniques", as taught by Hutchison (paragraph [0025]) and "protecting such data within a copier, or more broadly, within any system in which image data is scanned and retained for subsequent printing", as taught by Hutchison (paragraph [0003]).

- Hutchison does not disclose a file including:

  an unencrypted header with an identification of the scanned document.

McGraw discloses wherein transmitting the encrypted document with the hashed password includes transmitting a file including: an unencrypted header with an identification of the scanned document (e.g. fig. 4, abstract and col. 3, lines 6-11).

Hutchison and McGraw are analogous art because they are from the same field of endeavor of digital copier. At the time of the invention it would have been obvious to a person of ordinary skill in the art to incorporate McGraw's unencrypted header to Hutchison's method/system.

The motivation for doing so would have been since "The printed or viewed received FAX will have the unencrypted header at the top of the page so that the

receiving party (who may not be the intended recipient) will know to whom the received secure FAX document should be given to. For example a hotel's business center would need to know which guest the secure FAX should be delivered to", as taught by McGraw (col. 3, lines 6-11).

Response to Arguments

9. Applicant's argument filed 05 March 2007 have been respectfully and fully considered but they are not persuasive.

10. The amendment to claim 1 necessitate additional 112 (1^{st}) and (2^{nd}) rejections for claims 1-4 and 7-8.

11. Applicant's arguments are summarized as:

A. Cla ims 1, 9, 10, 19 have been amended to include the subject matter of claims 6 and 15..." as stated by the Applicant on page 7 of the remark, the examiner respectfully disagrees.

- First, the examiner respectfully points out that claims 9 and 19 are independent claims and both claims have no dependent claims and therefore, new ground of rejections are necessitated by the amendment for claims 9 and 19.

- Second, the examiner respectfully points out, in the **canceled claim 15**, it recited "...wherein the scanner transmits a file with **an unencrypted header including an identification of the scanned document and the hashed password, and encrypted document**

data". But in the **amended claims 10 and 19**, the claims 10 and 19 were amended as "...a file including **a header with an unencrypted identification of the scanned document and the hashed password, along with the encrypted document**...". The examiner carefully reviews the Applicant's original disclosure on page 9, lines 12-18, the Applicant discloses "...in Step 408, **more specifically means that the hashed password is transmitted with the encrypted document.** For example, **Step 408 may transmit a file including an unencrypted header with an identification of the scanned document, and the hashed password, along with encrypted document data**" and in fig. 4, step 408, "**transmitting encrypted document with password**" and step 410, "accepting encrypted document and password at printer".

B. Regard ing the Applicant's argument "The claimed invention recites the transmission of **hashed password which is included in the header along with an unencrypted identification of the encrypted document**. Once again, neither Hutchinson nor McGraw discloses the transmission of a hashed password in a file header, as recited in claims 1, 9, 10 and 19" on page 11 of the remark, the examiner respectfully disagrees.

- First, the examiner respectfully invites the Applicant to review the Examiner's response to argument item A above.

- Second, applicant argues that "**the transmission of hashed password which is included in the header along with an unencrypted identification of the encrypted document**". Instead, the claims 1, 9, 10 and 19 recite "**a file including a header with an unencrypted identification of an encrypted document and a hashed password, along with the encrypted document**" but not recites "**hashed password which is included in the header along with an unencrypted identification of the encrypted document**". Therefore, it is reminded that although the claims are interpreted in light of the specification, limitations from the specification are not read into claims. *See In re Van Geuns, 988 F. 2d 1181, 26 USPQ2d 1027*
- Third, the Applicant's disclosure does **not** explicitly define "a file including a header with an unencrypted identification of the scanned document and the hashed password, and encrypted document data" and "a file including a header with an unencrypted identification of an encrypted document and a hashed password, along with the encrypted document" as "a hashed password which is included in the header along with an unencrypted identification of the encrypted document", as the Applicant argues. Therefore, the claimed limitation should be given their broadest reasonable interpretation. In this case, the claimed limitations can be broadly

interpreted that hashed password resides in the file, not necessarily included in the header. The claimed limitations should not be limited to preferred embodiments in the specification. *See In re ACTV, Inc. v. The Walt Disney Company, 346 F.3d 1082, 1092, 68 USPQ2d 1516, 1524 (Fed. Cir. 2003) and In re E-Pass Technologies, Inc. v. 3Com Corporation, 343 F.3d 1364, 1368, 67 USPQ2d 1947, 1949 (Fed. Cir. 2003). (Fed. Cir. 1993)*

C. Regarding "..that the distribution of printing and scanning functions over multiple "boxes" cannot fairly be interpreted as evidence that Hutchinson suggests the transmission of encrypted documents with an accompanying password" on page 10 of the remark, the examiner respectfully disagrees.

- First, in paragraph [0014], Hutchison discloses "...**network-controlled** printer" and in paragraph [0013] and in fig. 2, Hutchison discloses "Fig 2 is a diagram of a set of digital copiers and associated computers arranged on **a network**..." And in paragraph [0029], Hutchison discloses "a plurality of digital copiers 10 are connected, through known means such as one or more subnetworks 72, 74 connected through a router 76..."
- Second, in paragraph [0021], Hutchison discloses "...In particular, the method known as "Pretty Good Privacy" or "PGP" uses a "**session key**"...which is itself encrypted using a public key and **sent** to a recipient..." and in paragraph [0025], Hutchison discloses "PGP then creates the session key, which is a random number typically derived from incidental data" and "In a sense, an entered

password or other identification is a type of incidental data useful in random number generation" in the paragraph [0025] of Hutchison.

D. Regarding "However, even if this statement were correct, it does not explain how an expert in the art could have modified the Hutchinson reference in such a way as to describe the claimed invention..." in pages 11-12, the examiner respectfully disagrees.

- First, the examiner respectfully points out the Applicant states "an expert in the art" is an error. The test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference; nor is it that the claimed invention must be expressly suggested in any one or all of the references. Rather, the test is what the combined teachings of the references would have suggested to those of **ordinary skill** in the art. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981).
- Second, In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, as stated in the record, Hutchison and McGraw are analogous art because **they are from the same field of endeavor of digital copier**. At the time of the invention it would have been obvious to a person of

ordinary skill in the art to **incorporate** McGraw's unencrypted header to Hutchison's method/system. The motivation for doing so would have been since "The printed or viewed received FAX will have the unencrypted header at the top of the page **so that the receiving party (who may not be the intended recipient) will know to whom the received secure FAX document should be given to**. For example a hotel's business center would need to know which guest the secure FAX should be delivered to", as taught by McGraw (col. 3, lines 6-11). Please note the examiner never uses the word "modify" in the prior Office Action.

Conclusion

12. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to April Y. Shan whose telephone number is (571) 270-1014. The examiner can normally be reached on Monday - Friday, 8:00 a.m. - 5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

10 May 2007
AYS

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100